Federal Housing Finance Agency
Office of Inspector General

FHFA Should Document Its Updated Procedure Requirement for Implementing Binding Operational Directives for IT Security

Compliance Review • COM-2025-003 • January 22, 2025

EXECUTIVE SUMMARY

PURPOSE

The Department of Homeland Security (DHS) issues Binding Operational Directives (BODs) to federal executive branch departments and agencies to ensure that they safeguard their information and information systems. In response to a Federal Housing Finance Agency (Agency or FHFA) Office of Inspector General (OIG) audit report recommendation, the Agency issued the Binding Operational Directives Procedure (Procedure) in 2022 to enhance its capacity to implement BODs. This compliance review assessed FHFA's implementation of Procedure requirements for BODs issued from January 1, 2023, through July 31, 2024 (review period).

RESULTS

During our review period, DHS issued one BOD in June 2023. That BOD required federal departments and agencies to take steps to protect networks with specified vulnerabilities from unauthorized intrusions via the Internet. We reviewed four Procedure requirements in the context of this BOD and tested three of them.

The Procedure first requires that FHFA information system staff consult with each other and the Chief Information Security Officer (CISO) to determine who will lead the Agency's response to every BOD received. FHFA modified this requirement so that the same IT specialist will lead all of the Agency's BOD responses. However, FHFA did not document the modification, which raises the risk of an ad hoc response by FHFA to BODs, as we found in our 2022 audit report.

The Procedure also requires that FHFA document any instances where it is unable to implement BOD requirements. FHFA determined this to be inapplicable because the Agency does not have any networks that fall within the June 2023 BOD scope. As a result, we did not perform testing on this second Procedure requirement.

Further, the Procedure requires that FHFA maintain BOD-related records – such as relevant emails – on the Agency's information system. We found that the Agency met this requirement.

Finally, the Procedure requires that FHFA maintain applicable BOD records for seven years in accordance with its Comprehensive Records Schedule. We found that the Agency complies with this requirement.

Recommendation

We recommend that FHFA revise the Procedure to reflect its current approach to determining who will lead the Agency's response to BODs and document any exceptions. The Agency agreed with our recommendation.

This report was prepared by Patrice Wilson, Senior Investigative Evaluator; and Wesley Phillips, Senior Policy Advisor. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to this report's preparation. This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website and www.oversight.gov.

Brian W. Baker
Deputy Inspector General, Office of Compliance

TABLE OF CONTENTS

ABBREVIATIONS

Agency or FHFA	Federal Housing Finance Agency
BOD	Binding Operational Directive
CISA	Computer Information Security Agency
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
IT	Information Technology
OCIO	FHFA Office of the Chief Information Officer
OIG	FHFA Office of Inspector General
Procedure	Binding Operational Directives Procedure
Review period	January 1, 2023, to July 31, 2024

BACKGROUND

Binding Operational Directives

A BOD is a compulsory directive to federal executive branch departments and agencies for safeguarding federal information and information systems. Pursuant to the Federal Information Security Modernization Act of 2014, DHS develops and issues BODs, then oversees federal agencies' implementation of them. Like other federal agencies, FHFA must comply with BODs.

Our 2022 Audit Found That FHFA Did Not Have a Policy for Implementing BODs

In a 2022 audit, we assessed FHFA's compliance with three select BODs issued from October 1, 2020, through September 30, 2021.[1] We determined that FHFA did not develop and maintain documented policies and procedures governing the process of implementing DHS BODs and relied instead on an informal undocumented process. We observed that without documented policies and procedures, FHFA might "respond to BODs in an ad-hoc, reactive manner."

We recommended that FHFA's Chief Information Security Officer (CISO) "develop and maintain policies and procedures for implementing DHS BODs."[2] FHFA agreed with the recommendation.

In 2022, FHFA Issued a Procedure to Implement BODs

On November 1, 2022, FHFA issued a Procedure containing the following four requirements:

- Upon receipt of a BOD, security staff in the FHFA [Office of the Chief Information Officer (OCIO)][3] must consult with the CISO to determine who will take the lead to assess the BOD's requirements and determine subsequent actions, including whether support from other [OCIO] divisions is necessary;
- Any exceptions made by FHFA when implementing the BOD's requirements (i.e., requirements that FHFA determined were not achievable) must be documented and approved by the CISO;

---

[1] OIG, *FHFA Did Not Fully Comply with DHS Binding Operational Directives for Securing Its Public Websites and Publishing Its Vulnerability Disclosure Policy* (AUD-2022-010) (August 31, 2022).

[2] The report contained two other recommendations that are not within this compliance review's scope.

[3] The Procedure refers to this office by its former designation, the Office of Technology and Information Management. We understand that, as of November 11, 2024, FHFA has renamed it the Office of the Chief Information Officer (OCIO). This report uses the office's updated name and acronym at FHFA's request and to avoid potential confusion going forward.

- The Agency must retain applicable records on its shared drive; and
- The Agency must retain applicable BOD records for seven years in accordance with FHFA's Comprehensive Records Schedule.

Based on the Agency's issuance of the Procedure, we closed the recommendation on December 29, 2022.

OBJECTIVE AND SCOPE

Our objective was to assess FHFA's compliance with the four selected Procedure requirements for any BOD issued from January 1, 2023, through July 31, 2024 (review period).

RESULTS

DHS Issued One BOD During the Review Period

On June 13, 2023, DHS issued BOD-23-02: Mitigating the Risk from Internet-Exposed Management Interfaces.[4] This was the only BOD issued during our review period. BOD-23-02 is intended to ensure that Agencies take steps to protect any of their networks that may be accessible via the public Internet. According to the BOD, in some cases, unauthorized users have accessed and compromised federal networks that lacked adequate protections.

The BOD also states that the Computer Information Security Agency (CISA) scans federal websites to detect networks that fall within the BOD's scope and, when it detects such a network, notifies the applicable federal department or agency.[5] The BOD requires that, within 14 days of either CISA's notification to a federal department or agency that one of its networks falls within the BOD's scope or the agency's self-detection of any such network, the exposed components must be removed from the Internet. Alternatively, the federal department or agency must take other steps to mitigate the risks associated with that network's continued accessibility via the Internet.

[4] See BOD-23-02 for additional information.

[5] CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

FHFA Did Not Update One Procedure Requirement but Complied with Other Applicable Requirements

FHFA Has Not Updated the Procedure to Reflect a Modification as to Who Will Lead the Agency's Responses to BODs

The Procedure states that upon receipt of a BOD, OCIO security staff will consult with the CISO regarding who will lead the Agency's response. FHFA officials said the requirement has been modified in practice. Specifically, they said FHFA has designated one Principal IT Specialist within the security staff to lead the response to all BODs rather than a consultation taking place among the security staff and the CISO to make the decision.[6] As of this writing, the Procedure has not been updated to reflect this modification.

Modifying policies in practice without documenting the modifications raises the risk we identified in our 2022 audit report that the Agency's undocumented processes could result in the ad hoc implementation of BODs.

Recommendation

FHFA should revise the Procedure to reflect its current approach in determining who will lead the Agency's responses to BODs and document any exceptions.

FHFA Did Not Identify Any Exceptions to BOD-23-02's Implementation Because the Agency Determined that the BOD's Requirements Do Not Apply

The second selected Procedure requirement mandates that any exceptions to the BOD's requirements (i.e., requirements that FHFA determined were not achievable) must be documented and approved by the CISO.

On June 13, 2023, which was the same day DHS issued BOD-23-02, the Principal IT Specialist emailed two OCIO network engineers to solicit input as to whether the Agency had any networks that fell within the scope of the BOD (i.e., that were accessible from the public Internet). The engineers confirmed that the Agency did not have any such networks.[7]

In August 2024, CISA notified FHFA that its scan of the Agency's system had potentially identified networks that fell within the scope of BOD-23-02. The Principal IT Specialist notified

[6] Consistent with the Agency's revised practice, this Principal IT Specialist led the response to BOD-23-02.

[7] On June 14, 2023, FHFA, as a management control, also updated its System and Communications Protection Standard to reflect the requirements in BOD-23-02. The standard defines the security requirements the Agency has put in place to accomplish system and communication protection for information being transmitted, received, stored, and managed. The updates included the language from BOD-23-02 stating that networks cannot be accessible from the public Internet.

CISA later that day that the scan result was a "false positive" and that the Agency did not have any networks that fell within the scope of the BOD. Several days later CISA notified FHFA that it accepted the Agency's representations.

FHFA officials told us that because the Agency does not have any networks that fall within BOD-23-02's scope, the Procedure's exception requirement did not apply to the Agency. As a result of the BOD's inapplicability to FHFA, we were unable to perform testing of this second Procedure requirement. We note, however, that the Agency promptly took the necessary steps to determine BOD-23-02's applicability.

FHFA is Maintaining Applicable Records as Required

The third selected Procedure requirement mandates that the Agency retain applicable records on the shared drive. Our testing of FHFA documentation determined that the Agency is maintaining records for BOD-23-02 – such as internal OCIO email and correspondence with CISA – on the shared drive as required.

The fourth selected Procedure requirement is that FHFA maintain applicable records for BOD-23-02 for seven years in accordance with Comprehensive Records Schedule. An FHFA official said that the Agency has maintained documents for BOD-23-02 as required. We found that the Agency is complying with this requirement.

FHFA COMMENTS AND OIG EVALUATION.....

We provided a draft of this report to FHFA for its review and comment. The Agency's comments are included in the Appendix to this report. FHFA states that it agrees with the recommendation and that by February 15, 2025, OCIO will update the Procedure to designate the Chief, Cybersecurity Incident Management, Operations, and Forensics Section, as the role responsible for managing BODs. We will close the recommendation upon reviewing the documentation that FHFA committed to provide.

APPENDIX I: METHODOLOGY

We initiated this compliance review to assess FHFA's compliance with the Procedure for any BOD issued from January 1, 2023, through July 31, 2024 (the review period). To do so, we reviewed Agency documentation pertaining to its implementation of BOD-23-02. We also interviewed Agency officials responsible for BOD-23-02's implementation.

We conducted our compliance review from September 2024 through October 2024 under the authority of the Inspector General Act of 1978, as amended, and in accordance with the *Quality Standards for Inspection and Evaluation* (December 2020), which were promulgated by the Council of the Inspectors General on Integrity and Efficiency.

We provided FHFA with a draft of this report for its review and comment. We have taken the Agency's feedback into account.

APPENDIX II: FHFA MANAGEMENT RESPONSE.....

This page intentionally blank. See the following page(s).

Federal Housing Finance Agency

MEMORANDUM

TO: Brian Baker, Deputy Inspector General Office of Compliance

THRU: Gina Cross, Chief Operating Officer

GINA CROSS Digitally signed by GINA CROSS Date: 2025.01.08 14:05:57 -05'00'

FROM: Luis Campudoni, Chief Information Officer

LUIS CAMPUDONI Digitally signed by LUIS CAMPUDONI Date: 2025.01.13 07:18:39 -05'00'

SUBJECT: Draft Compliance Report: FHFA Should Document Its Updated Procedure Requirement for Implementing Binding Operational Directives for IT Security

DATE: January 8, 2025

Thank you for the opportunity to respond to the above-referenced draft compliance report (Report) by the Office of Inspector General (OIG), which contains one recommendation. This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the recommendation, which is being managed by the Office of Chief Information Officer (OCIO).

Recommendation 1: *FHFA should revise the Procedure to reflect its current approach in determining who will lead the Agency's responses to BODs and document any exceptions.*

FHFA's Recommendation 1 Response: FHFA agrees with Recommendation 1. OCIO will update its Binding Operational Directives (BOD) Procedure to designate the Chief, Cybersecurity Incident Management, Operations, and Forensics Section as the role responsible for managing the BODs, by February 15, 2025.

If you have questions, please contact Stuart Levy at (202) 649-3610 or by e-mail at Stuart.Levy@fhfa.gov.

cc: Marcus Williams
Edom Aweke
Tom Leach
Jeff Harris
Brandon Davis
Ralph Mosios
Warren Hammonds

Federal Housing Finance Agency
Office of Inspector General

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write: FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219